RSAC 2025 Conference

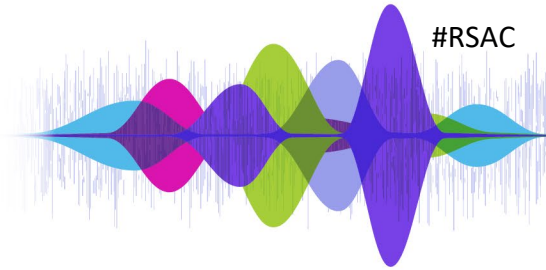
Many Voices.
One Community.

SESSION ID: HTA-T02

Adventures in the Underland: Uncommon Hacker's Persistence Methods

Paula Januszkiewicz

CEO and Founder, Microsoft MVP and RD
CQURE
www.linkedin.com/in/paulajanuszkiewicz



Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

Insightful Stats for 2025

$4.88M

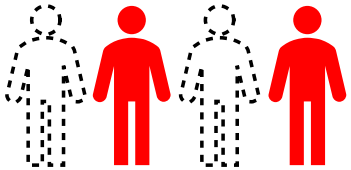
Is the global average cost of a data breach in 2024. It increased 10% over the previous year.

292 Days

That's how long on average it took to identify and contain breaches involving stolen or compromised credentials.

68%

of data breaches involved human error in 2024.



>50%

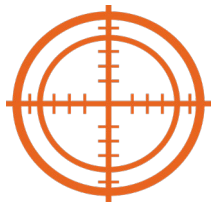
of breached organizations are facing high levels of security staffing shortages. That's a 26.2% increase from the prior year.

Source: IBM (2024), Verizon (2024)

Impactful Hacking Stats for 2025

43%

of all cyberattacks are aimed at small businesses.



95%

of data breaches are financially motivated.

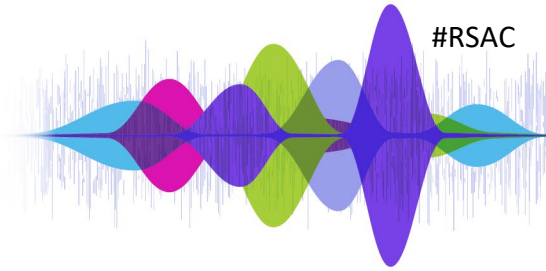
83%

of breaches involve external actors.

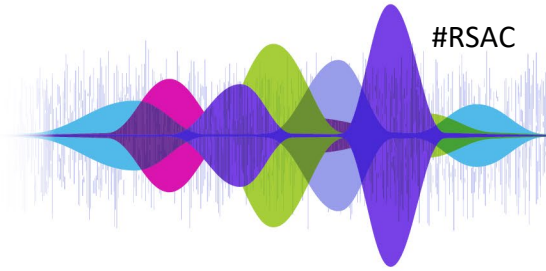
64%

of organizations do not have a cyber security incident response plan.

Source: Verizon (2023); Accenture (2023), Kroll (2022)



https://attack.mitre.org/tactics/TA0003/



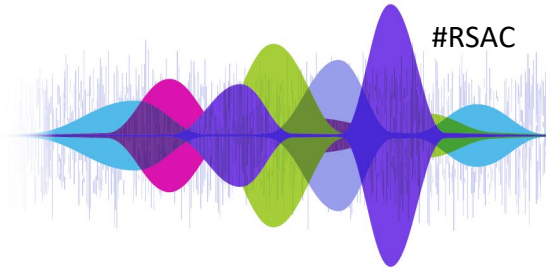
Types of Persistence: General Summary

Persistence Through Misconfiguration

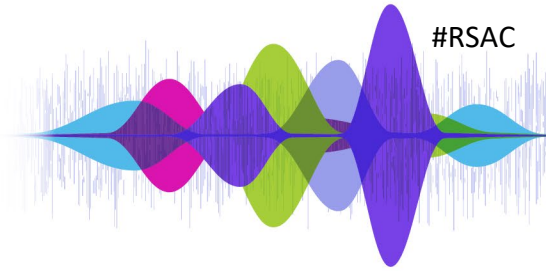
- **Key learning points:**
  - The best approach is to avoid using a solution until we know when it fails (time matters too)
  - Solution may have some ‘backdoor weakness’
  - Some antivirus solutions can be stopped by SDDL modification for their services
  - Passwords are stored in various configuration files / places
  - Lack of monitoring adds up -> Golden Ticket etc.
  - Privilege Access Management not in place
  - Example: How to get access to the password management portal?

Persistence Used by Malware

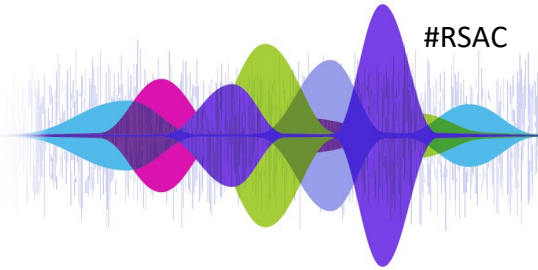
- **Key learning points:**
  - Persistence through Windows mechanisms (services, task scheduler etc.)
  - Autoruns / FRST are very helpful
  - Malware payload (e.g. powershell script) may be stored in registry
  - Malware as a debugger for other apps
  - Extension hijacking (e.g. *.txt files are opened with malware by default)
  - DLL hijacking attacks
  - Callback on shutdown
  - Adding entries to Group Policy
  - WMI repository
  - Domain persistence, like AdminSDHolder etc.



Warm-up:
Access or No Access?

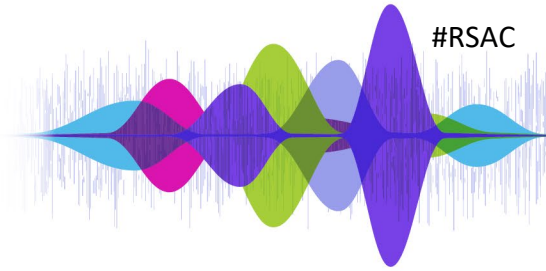


Persistence Through Windows Services

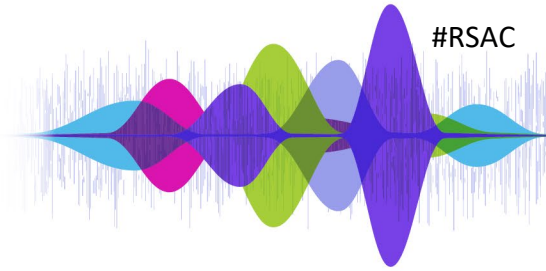


Service Configuration Mistakes

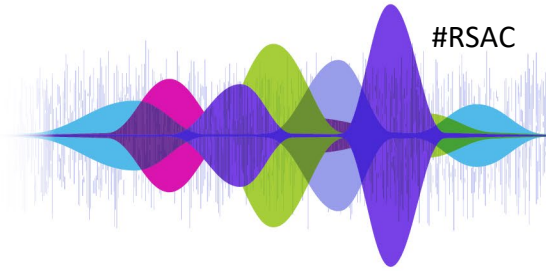
1. **Misconfigured service account:**
   a. Password stored in the registry
   b. Account is not denied all logon types, except for service logon type
   c. Account can log on to servers other than when it is configured
   d. Password never expires (depends on the risk assessment)
2. **Incorrect permissions to the service defining who can start or stop it**
3. **Incorrect permissions to the folder where the service executable is located**
4. **Unquoted service path**
5. **Usage of Service Principal Name, while using the weak service account password (Kerbroasting, SMB Relay)**



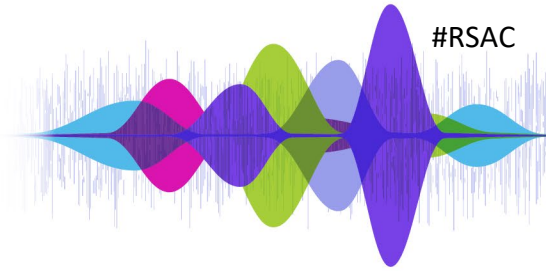
Persistence Through Phishing and WMI



Persistence Through MFA Violation

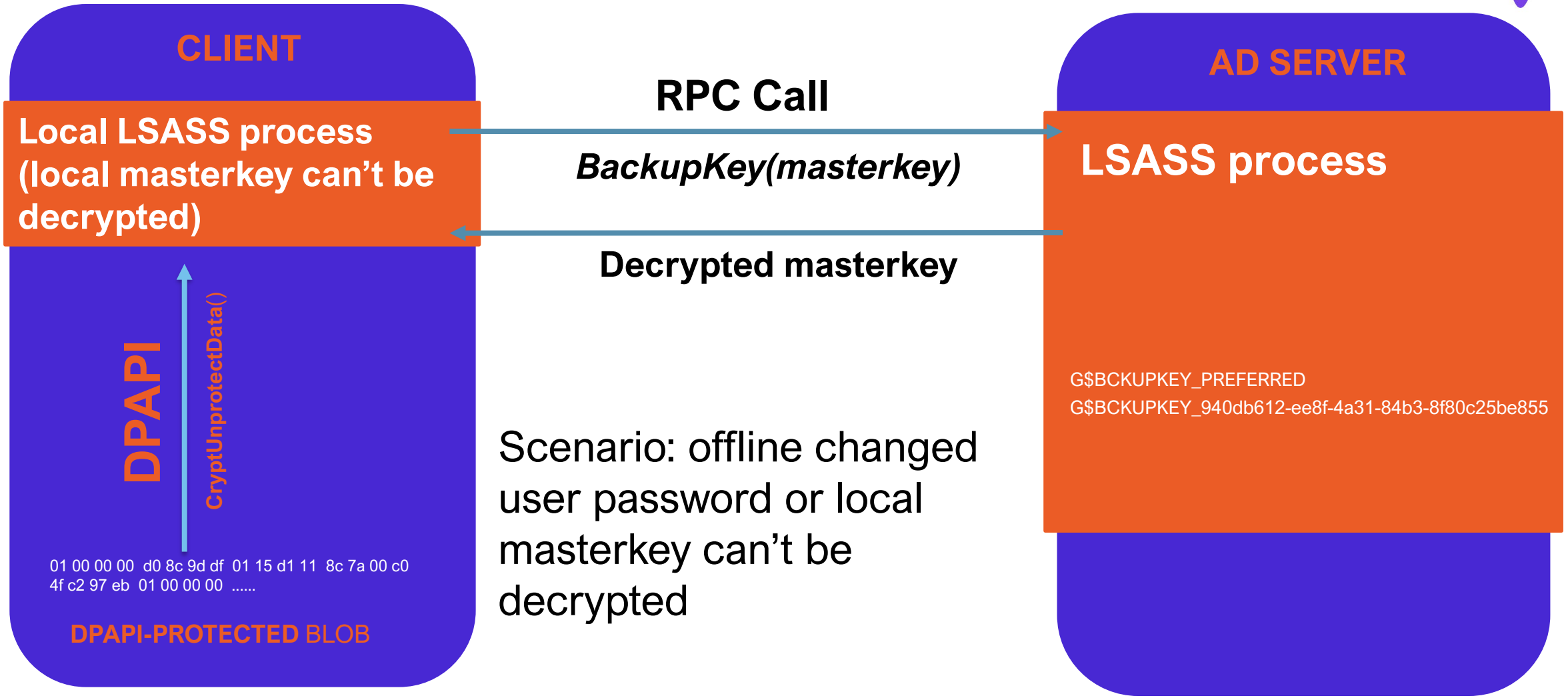


Persistence Through Privileged Access or… PKI?

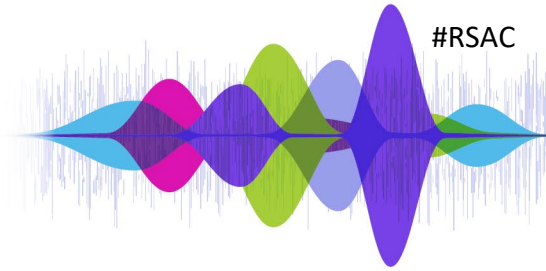


Persistence Through the Domain

DPAPI + AD



Scenario: offline changed user password or local masterkey can't be decrypted



Classic DPAPI Flow: Getting the user's secrets

Classic Data Protection API

- Based on the following components:

Password, data blob, entropy

- Is not prone to password resets!

Protects from outsiders when being in offline access

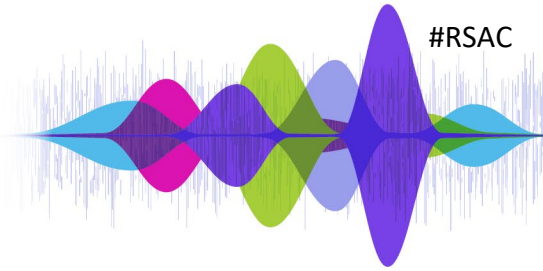
Effectively protects users data

- Stores the password history

You need to be able to get access to some of your passwords from the past

Conclusion: OS greatly helps us to protect secrets

Getting the User's Classic DPAPI Secrets



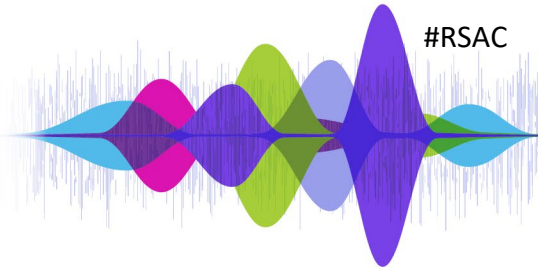
DPAPI (classic)

A. MasterKey
   1. pwdhash = MD4(password) or SHA1(password)
   2. pwdhash_key = HMACSHA1(pwdhash, user_sid)
   3. PBKDF2(…, pwdhash_key,…), another elements from the file. Windows 10 no domain: SHA512, AES-256, 8000 rounds
   4. Control – HMACSHA512

B. CREDHIST
   1. pwdhash = MD4(password) or SHA1(password)
   2. pwdhash_key = HMACSHA1(pwdhash, user_sid)
   3. PBKDF2(…, pwdhash_key,…), another elements from the file. Windows 10 no domain: SHA512, AES-256, 8000 rounds
   4. Control – HMACSHA512

C. DPAPI blob Algorithms are written in the blob itself.

Formatting of the cached logon data



MSDCC2

1. bootkey: classes from HKLM\SYSTEM\CCS\Control\Lsa + [class names for: Data, GBG, JD, Skew1] (+arrays' permutations) int[] permutationBootKey = new int[] { 0x8, 0x5, 0x4, 0x2, 0xb, 0x9, 0xd, 0x3, 0x0, 0x6, 0x1, 0xc, 0xe, 0xa, 0xf, 0x7 };
2. PolEKList: HKLM\SECURITY\Policy\PolEKList [default value]
3. lsakey: AES_DECRYPT(key, data) -> AES(bootkey, PolEKList)
4. NL$KM secret: HKLM\SECURITY\Policy\Secrets\NL$KM
5. nlkm_decrypted: AES_DECRYPT(lsakey, NL$KM secret)
6. Cache_Entry{id} -> HKLM\SECURITY\Cache\NL${id}
7. cache_entry_decrypted -> AES_DECRYPT(nlkm_decrypted, Cache_Entry{id})

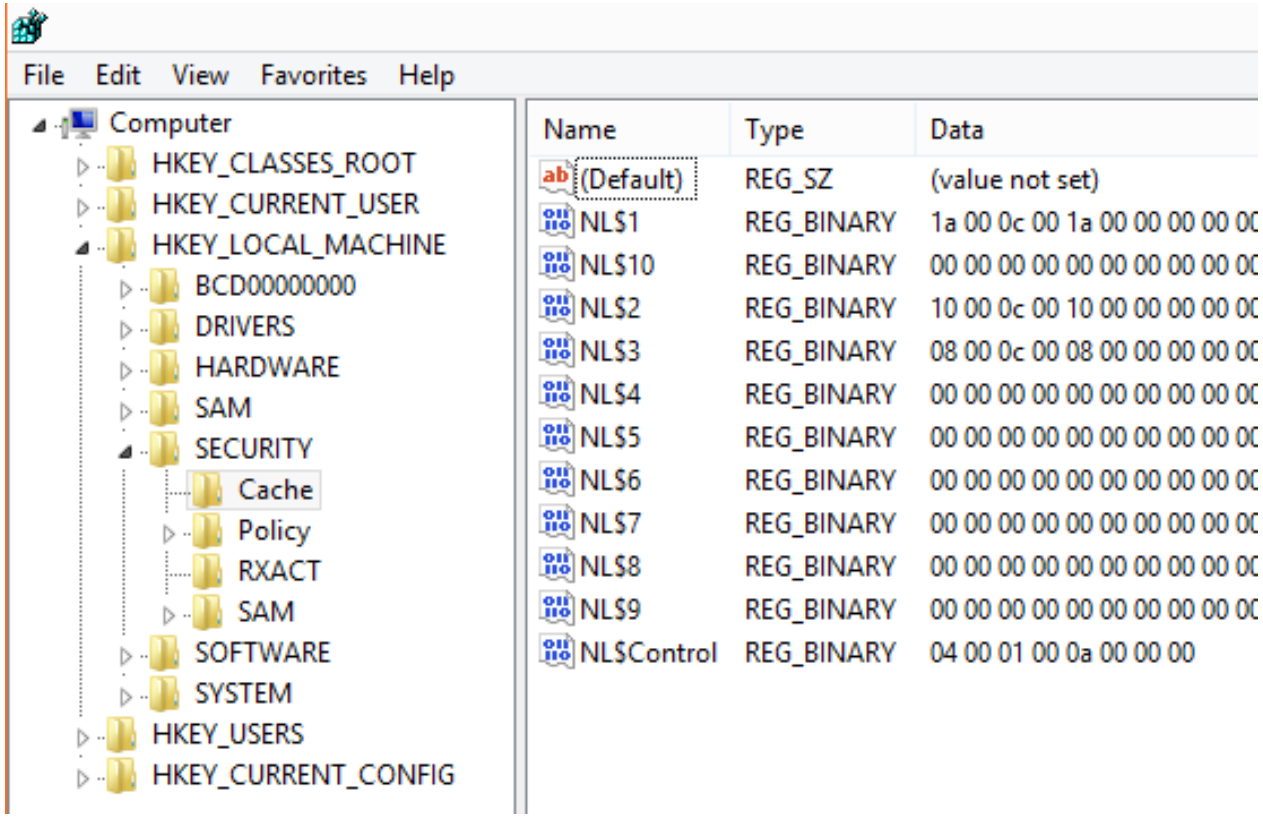
Cached Logons: Iterations

The number of iterations in PBKDF2, it is configurable through the registry:

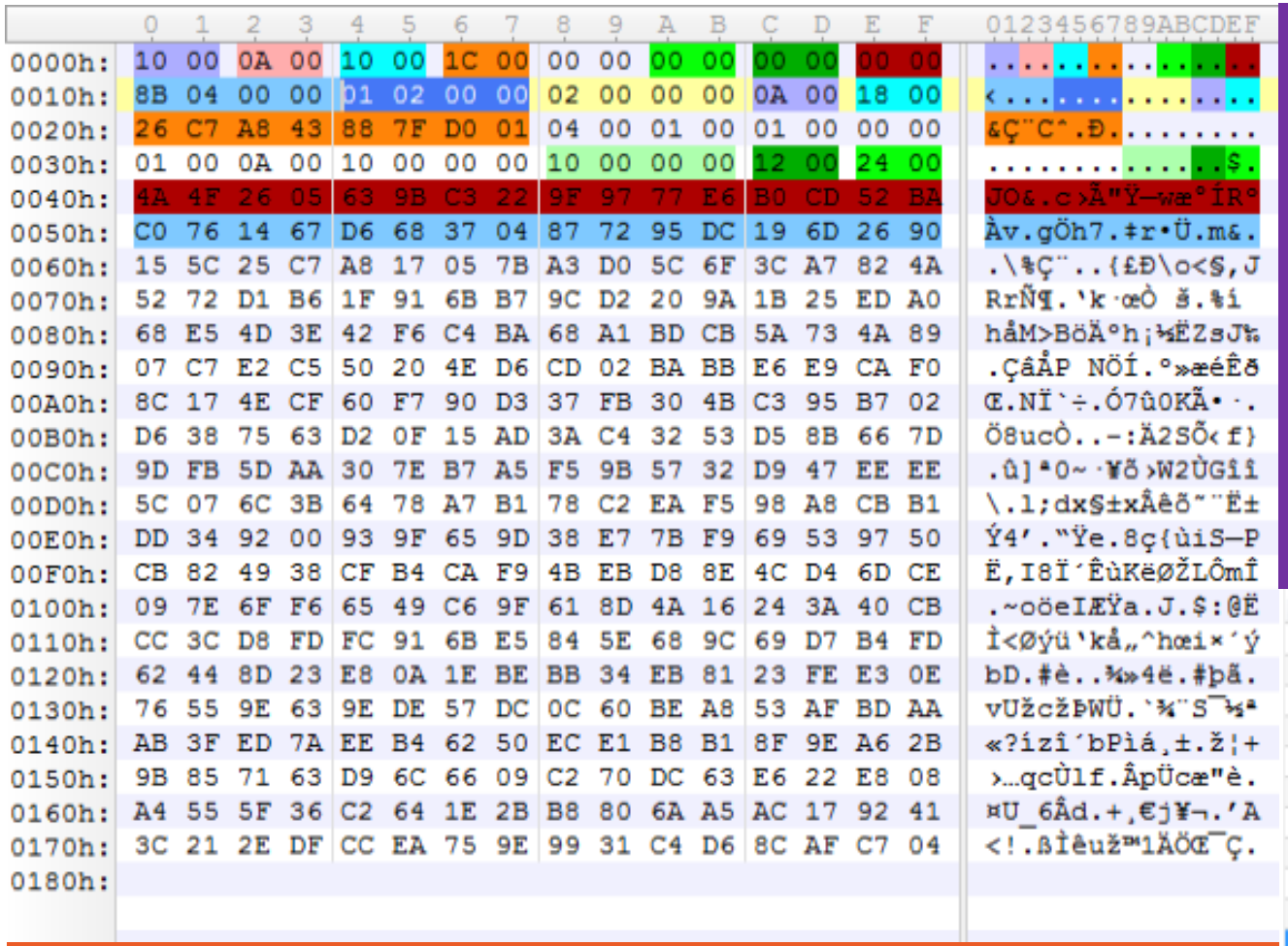
HKEY_LOCAL_MACHINE\SECURITY\Cache DWORD (32) NL$IterationCount

If the number is less than 10240, it is a multiplier by 1024 (20 therefore gives 20480 iterations)

If the number is greater than 10240, it is the number of iterations (rounded to 1024)


File Edit View Favorites Help
Computer
HKEY_CLASSES_ROOT
HKEY_CURRENT_USER
HKEY_LOCAL_MACHINE
BCD00000000
DRIVERS
HARDWARE
SAM
SECURITY
Cache
Policy
RXACT
SAM
SOFTWARE
SYSTEM
HKEY_USERS
HKEY_CURRENT_CONFIG
Name Type Data
(Default) REG_SZ (value not set)
NL$1 REG_BINARY 1a 00 0c 00 1a 00 00 00 00 00
NL$10 REG_BINARY 00 00 00 00 00 00 00 00 00 00
NL$2 REG_BINARY 10 00 0c 00 10 00 00 00 00 00
NL$3 REG_BINARY 08 00 0c 00 08 00 00 00 00 00
NL$4 REG_BINARY 00 00 00 00 00 00 00 00 00 00
NL$5 REG_BINARY 00 00 00 00 00 00 00 00 00 00
NL$6 REG_BINARY 00 00 00 00 00 00 00 00 00 00
NL$7 REG_BINARY 00 00 00 00 00 00 00 00 00 00
NL$8 REG_BINARY 00 00 00 00 00 00 00 00 00 00
NL$9 REG_BINARY 00 00 00 00 00 00 00 00 00 00
NL$Control REG_BINARY 04 00 01 00 0a 00 00 00

Encrypted Cached Credentials: Legend



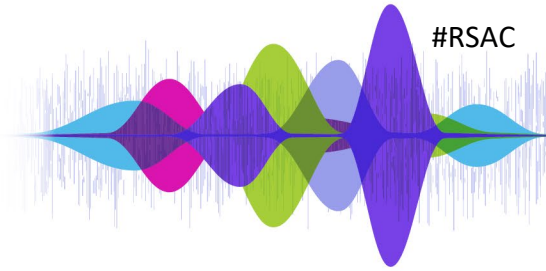
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
0000h:	10	00	0A	00	10	00	1C	00	00	00	00	00	00	00	00	00	.....
0010h:	8B	04	00	00	01	02	00	00	02	00	00	00	0A	00	18	00	‹.....
0020h:	26	C7	A8	43	88	7F	D0	01	04	00	01	00	01	00	00	00	&Ç¨Cˆ.Ð.....
0030h:	01	00	0A	00	10	00	00	00	10	00	00	00	12	00	24	00	.....$.
0040h:	4A	4F	26	05	63	9B	C3	22	9F	97	77	E6	B0	CD	52	BA	JO&.c›Ã"Ÿ—wæ°ÍR°
0050h:	C0	76	14	67	D6	68	37	04	87	72	95	DC	19	6D	26	90	Àv.gÖh7.‡r•Ü.m&.
0060h:	15	5C	25	C7	A8	17	05	7B	A3	D0	5C	6F	3C	A7	82	4A	.\%Ç¨..{£Ð\o<§,J
0070h:	52	72	D1	B6	1F	91	6B	B7	9C	D2	20	9A	1B	25	ED	A0	RrÑ¶.'k·œÒ š.%í
0080h:	68	E5	4D	3E	42	F6	C4	BA	68	A1	BD	CB	5A	73	4A	89	håM>BöÄºh¡½ËZsJ‰
0090h:	07	C7	E2	C5	50	20	4E	D6	CD	02	BA	BB	E6	E9	CA	F0	.ÇâÅP NÖÍ.º»æéÊð
00A0h:	8C	17	4E	CF	60	F7	90	D3	37	FB	30	4B	C3	95	B7	02	Œ.NÏ`÷.Ó7û0KÃ•·.
00B0h:	D6	38	75	63	D2	0F	15	AD	3A	C4	32	53	D5	8B	66	7D	Ö8ucÒ..-:Ä2SÕ‹f}
00C0h:	9D	FB	5D	AA	30	7E	B7	A5	F5	9B	57	32	D9	47	EE	EE	.û]ª0~·¥õ›W2ÙGîî
00D0h:	5C	07	6C	3B	64	78	A7	B1	78	C2	EA	F5	98	A8	CB	B1	\.l;dx§±xÂêõ˜¨Ë±
00E0h:	DD	34	92	00	93	9F	65	9D	38	E7	7B	F9	69	53	97	50	Ý4'."Ÿe.8ç{ùiS—P
00F0h:	CB	82	49	38	CF	B4	CA	F9	4B	EB	D8	8E	4C	D4	6D	CE	Ë‚I8Ï´ÊùKëØŽLÔmÎ
0100h:	09	7E	6F	F6	65	49	C6	9F	61	8D	4A	16	24	3A	40	CB	.~oöeIÆŸa.J.$:@Ë
0110h:	CC	3C	D8	FD	FC	91	6B	E5	84	5E	68	9C	69	D7	B4	FD	Ì<Øýü'kå„^hœi×´ý
0120h:	62	44	8D	23	E8	0A	1E	BE	BB	34	EB	81	23	FE	E3	0E	bD.#è..¾»4ë.#þã.
0130h:	76	55	9E	63	9E	DE	57	DC	0C	60	BE	A8	53	AF	BD	AA	vUžcžÞWÜ.`¾¨S¯½ª
0140h:	AB	3F	ED	7A	EE	B4	62	50	EC	E1	B8	B1	8F	9E	A6	2B	«?ízî´bPìá¸±.ž¦+
0150h:	9B	85	71	63	D9	6C	66	09	C2	70	DC	63	E6	22	E8	08	›…qcÙlf.ÂpÜcæ"è.
0160h:	A4	55	5F	36	C2	64	1E	2B	B8	80	6A	A5	AC	17	92	41	¤U_6Âd.+¸€j¥¬.'A
0170h:	3C	21	2E	DF	CC	EA	75	9E	99	31	C4	D6	8C	AF	C7	04	<!.ßÌêuž™1ÄÖŒ¯Ç.
0180h:																	

Name	Value	Start	Size	Color	Comment
struct Header h		0h	96	Fg: Bg:	
ushort uname_len	16	0h	2	Fg: Bg:	
ushort domain_len	10	2h	2	Fg: Bg:	
ushort mail_nick_len	16	4h	2	Fg: Bg:	
ushort cn_len	28	6h	2	Fg: Bg:	
ushort u1	0	8h	2	Fg: Bg:	
ushort logon_script_len	0	Ah	2	Fg: Bg:	
ushort profile_path_len	0	Ch	2	Fg: Bg:	
ushort home_dir_len	0	Eh	2	Fg: Bg:	
uint user_sid	1163	10h	4	Fg: Bg:	
uint primary_group_id	513	14h	4	Fg: Bg:	
uint u2	2	18h	4	Fg: Bg:	
ushort group_sids_len	10	1Ch	2	Fg: Bg:	
ushort domain_netbios_name...	24	1Eh	2	Fg: Bg:	
FILETIME last_local_logon	04/25/2015 18:47:22	20h	8	Fg: Bg:	
ushort u3	4	28h	2	Fg: Bg:	
ushort u4	1	2Ah	2	Fg: Bg:	
uint u5	1	2Ch	4	Fg: Bg:	
ushort u6	1	30h	2	Fg: Bg:	
ushort u7	10	32h	2	Fg: Bg:	
uint u8	16	34h	4	Fg: Bg:	
uint u9	16	38h	4	Fg: Bg:	
ushort domain_name_len	18	3Ch	2	Fg: Bg:	
ushort email_len	36	3Eh	2	Fg: Bg:	
byte iv[16]	JO&|c›Ã"Ÿ—wæ°ÍR°	40h	16	Fg: Bg:	

Encrypted Cached Credentials

DK = PBKDF2(PRF, Password, Salt, c, dkLen)

Microsoft's implementation: MSDCC2= PBKDF2(HMAC-SHA1, DCC1, username, 10240, 16)



Persistence Through Old & Default

Persistence Through Old Defaults

- **Key learning points:**
  - SNMPv3 addresses: user-based system for access control, a means to properly authenticate users, and a method for encrypting SNMP traffic between agent and host
  - SQL issues – TDS provides by default lack of encryption
  - ODBC Driver – check if it has a secure networking layer built into it

Persistence & Countermeasures: Summary

- First and foremost, prevent unwanted programs from running
- Block file writes to unusual places, if possible, such as public user profile in Windows
- Reduce privileges so that more advanced persistence techniques fail due to missing privileges
- Regularly perform threat hunting activities
- Introduce strict monitoring of identity use
- Implement the strategy of auditing vendors

Apply What You Have Learned Today

- Next week you should:
  - Examine your organization's security logs and endpoint detection tools for unusual or persistent entries that might indicate hidden malware.
  - Simulate some of the uncommon persistence techniques demonstrated in the session to evaluate how well your current security tools and monitoring systems detect them.
- In the next three months following this presentation you should:
  - Develop and implement a more robust threat-hunting process focusing on identifying stealthy persistence mechanisms across endpoints and network infrastructure.
  - Update and test your organization’s incident response procedures to ensure they address advanced persistence techniques and ransomware threats effectively.

RSAC™ 2025 Conference

Many Voices.
One Community.